Afro Asian Journal of Social Sciences
Volume V, No 4. Quarter IV 2014
ISSN: 2229 – 5313

CYBER FRAUD, GLOBAL TRADE AND YOUTH CRIME BURDEN: NIGERIAN EXPERIENCE

Jegede Ajibade Ebenezer
Lecturer, Department of Sociology, Covenant University, Ota, Ogun State, Nigeria

ABSTRACT
This paper examines the relationship between modern technology and the multiplicity of fraud. Specifically, it argues that the involvements of sizeable Nigerians in crime is not empirically tied to their dispositions and psychopathologies, these attributes are widely believed to be responsible for getting one into trouble with the law, but it rather identifies the socio-economic deterioration mostly prevalent in the Nigeria society as the most explicable factor intensifying the participation of most Nigerian especially youths in cyber fraud. It borrows from the theoretical ideas of Derek Cornish and Ronald Clarke on the contributions of the environment to the incidence and the rising rate of crime globally. The paper finally proffers few pragmatic solutions to the problem of cyber fraud in the e-business environment.

Keywords: Youths, Internet, Fraud, Participation, Environment, Technology

Fraud and Technology: An Overview
Fraud is a generic term and embraces the multifarious means which human ingenuity can devise, which are resorted to by one individual to get an advantage over another by false representations. it includes surprise, trick, cunning, and unfair ways by which another is cheated (Singleton and Singleton, 2010:40). No definite and invariable rule can be laid down as a general proposition in explaining fraud. The boundaries demarcating fraud are those which limit human knavery (Webster, 1964). The most important to this paper is the aspect of fraud that affects technology as facilitator of crime. This form of fraud is a product of modernization on the one hand and globalization which culminated in advanced capitalism, on the other hand. As a matter of fact,

the urgency of finding a lasting solution to the problem of cyber fraud keeps calling per day, more importantly when one considers the magnitude of risk that online transactions portend for the world of business now and in the nearest future. In essence, a spontaneous projection and timely remediation of fraud related risks often mediated by the Internet becomes important.

Diverse research have concentrated efforts on the establishment of linkages between the human environment, increasing nature of technological driven business transactions, the growth of fraud and the attendant skepticism revolving around the security of online interaction globally. In one of such studies, Kovacich (2008:4) reveals that trade on a global scale has been increasing for centuries, and it is expected to continue to increase, in some areas expanding exponentially and more rapidly than in the past. Consequently, drawing an inference from the findings of Forrester Research (2001) and situating Kovacich's observation in the context of its findings, it was earlier predicted that between 2001 and 2006, $1 trillion worth of goods and services worldwide would be purchased online or influenced by information found about product and services.

This projected figure appears enormous and its realization is expected to be facilitated by the Internet thus invariably raising a concern about the volume of financial burden and risk disposable factors inherent in e-business arena Similarly, when one considers the mode and magnitude of online payment and the current dimension of acquiring goods and services globally, it is vividly clear that most nations will be forced to glue to the Internet or at best online trading in the foreseeable future. The realization of this prediction places nations at a vantage point of risks. In the US. for instance, trading often takes place mainly in the form of credit and debit cards, while in Europe, Asia and Africa payment and reception of goods and services takes place through bank or money transfers and cash delivery (Montague, 2011:25).

Quantifying the implications of these forms of payment as relating to transactions worldwide, it may be succinctly mentioned that cyber fraud business may as well enjoy more days of operations if adequate measures are not taken to arrest its tide. Most people and even most researchers believe that fraud is on the increase both in size and frequency; it is difficult to know for sure (Dutton and Helsper, 2009). Information on the magnitude of fraud often comes from

four sources: governments, researches, insurance companies and fraud victims (Albrecht et al, 2012:5). Although, the true picture of losses to Internet fraud is nearly non-existent in Nigeria. A 2008 research estimates shows that U.S. organizations lose roughly 7 percent of their annual revenues to fraud. Quantifying this in terms of ratio to the gross domestic product, this (7 percent) figure would translate into approximately $994 billion in fraud losses—in the United States alone.

Along the same line of reasoning, Fischer (2007), a German Foreign Minister, estimated that cyber crime cost Germany well over $40 billion a year. This revelation remains worrisome in terms of the magnitude of losses attributable to cyber fraud. Apart from the monetary losses to nations of the world, a thorough research estimate must by right take cognizance of the fraud consequences involved in the social costs of crime. This will include its cost to the criminal justice system with its potential of draining taxpayer money and the cost of fraud needed to replace stolen/damaged property occasioned by such crime. There is also the need to evaluate the costs of fraud to the victim which entails reduced productivity, health expenses and socio-psychological shock.

Just as the international business is growing along with fraud activities, there is an attendant growth in the population of net fraudsters. It then becomes a challenge for governments, organizations and private individuals to take far reaching steps that will neutralize the risks associated with on line fraud. Therefore, this paper on fraud is divided into four sub-sections. The first considers what fraud is with the major emphasis on what cyber fraud is all about; the second attempts the theoretical explanation to youth fraud involvement in Nigeria while the third critically looks at the evolution of cyber fraud and, finally, the fourth discusses the general nature of cyber fraud and youths participation and closely followed by measures to be taken to arrest the tide.

Conceptualizing Fraud

There are diverse definitions of fraud but each focuses on a particular aspect of fraud bearing its strength from the context examined. Apart from the diversity inherent in defining fraud, such an

exercise is equally complicated by the beliefs and values of those analyzing any typology of behaviour in determining its quality as either fraudulent or not. The motivations behind fraud vary by type of fraud, as well as by individual case. In general, the overall reason behind committing fraud is for financial gain or incentive. In some cases it may be for face saving (Pedneaut, 2009:19). Black's Law Dictionary (2004) conceives of fraud as a knowing misrepresentation of the truth or a concealment of a material fact to induce another to act to his or her detriment. A misrepresentation made recklessly without belief in its truth to induce another person to act. It fundamentally rests on deception and fraudulent behaviour which includes acts in which individuals construct lies or misrepresentations, as well as acts in which individuals unexpectedly conceal information from another (Ekman 1985). Simply put, it is an intentional false statement used to deprive an innocent victim of money or property (Well, 2010). In relation to cyber or Internet fraud, the US Department of Justice Internet Fraud Center defines Internet fraud as ―any type of fraud scheme that uses one or more components of the Internet – such as chat rooms, e-mail, message boards or website—to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

It was reported that credit card and access device frauds are most common globally. This is due to the fact that criminals take advantage of access device because of its simplicity, acceptability and because it contains information for a variety of consumer uses in the world of business. Credit card serves as a means of settling payments in both local and international business and both facilities serve as means of transaction without restrictions across socio-cultural borders. The major driver of these fraud types remains the Internet which is located in the computer age.
Considering the types of fraud, the list of fraud is endless but amenable to the area of interest of any researcher. A single research work cannot explain the variants of fraud available in our modern technologically driven society. The difficulty in accomplishing this is related to the nature or attributes of each type on the one hand, and the ingenuity and sophistication required by the perpetrators of fraud to achieve a successful fraudulent outcome on the other hand. Bank fraud, bankruptcy, constructive fraud, extrinsic fraud, fraud in law, fraud in inducement, fraud on the community, fraud on the court, fraud on the market, fraud on the patent office, insurance

fraud, intrinsic fraud, long-firm fraud, mail fraud, promissory fraud, wire fraud are all part and parcel of the fraud package existent in the modern e-business environment. Fraudulent alienation, fraudulent banking, fraudulent conveyance are not also exempted. Fraud results in disappointing outcome and promotes disillusionment to victims in their future decisions to participate in trust laden relationships.

Theoretical Anchorage of Fraud Participation in Nigerian Society

Resituating the Nigerians-crime nexus, representing the near general view of most nationals of the advanced capitalist nations such as America, UK, and other European nations, the challenges precipitating crime event among Nigerian people is not tied to criminal dispositions or psychopathologies often blamed for such participations. The fact remains that both potential and practicing criminals are affected by Nigerian society. The inducible factors propelling participation in crime are endemic in the Nigeria's socio-economic environment and their effects are also evenly distributed among Nigerian people.. There is a correlation between this current view and the postulations of other earlier researchers (Clarke and Martin, 1975; Clarke and Cornish, 1983, 1986). The Nigerian society provides both cues and reinforcement in crime participation. By implication, these situational variables are knitted with primary and secondary precipitators which exist side by side in this regard. At the primary surface, opportunity for crime exists due to many factors inherent in Nigeria's economic environment: so also is the prevalence of corruption ridden practices. The secondary precipitator is firmly located in the immediate crisis affecting most crime participants. The latter in most cases jumpstarts crime participants into a collision course with the law. The combination of both precipitators can be linked to the Nigerian condition. This condition consists of unimaginable economic vulnerabilities located in the virtual disappearance of survivable climate for vast majority of Nigerian people on one hand and the rising profile of corrupt laden practices both implicating the citizenry and government officials, on the other hand. Consequently, Nigeria's environment is therefore consistent with repeated experimentation with all manner of crime knowable globally. Basically, this 'environment' also encompasses human lifestyles, motives, needs and attractable inducers propelling goal pursuit and attainments within which crime participation in this context becomes a rational response. This position is supported by the fact that a typology of culture had evolved

which gives credence to learning and imbibing the philosophy of circumventing known standards tailored towards forestall undesired consequences though when negative. Using 'ones head' to get one's goal achieved then becomes the duty of an average Nigerian. This does not exclude the use of all shade of illicit methods to get what is germane to the survival of individuals. The role of this unique rational decision making on the part of diverse Nigerians (mostly youths) have been viewed as the most probable factor in crime and fraud participation (Clark and Cornish, 1983). In this regard, youths are often at a cross road on whether to continue to hope for a better future but yet being confronted with socio-economic challenges inherent in Nigeria's socio-material environment on one hand or to opt for the immediate solution to their current predicament while damning the consequences of punishments on the other hand. Fraudsters in most cases identify their targets, plan their activities, put into use the required tact to reach out to their victims and apply concerted efforts to avoid detection, and then squirrel their fraud profits in some hidden bank accounts (Siegel, 2008). Theoretically, this calculated action of fraudsters suggests that decision to commit crime involve both rational, detailed planning and decision making designed to maximize personal gain and avoid capture and punishment. Decisions to pick up career in the domain of fraud as an alternative to conventional profession and a means of cushioning the effects of socio-economic problems most prevalent in Nigeria Apart from the causal factor inherent in the structural challenges being faced in Nigeria, other reason intensifying the spread of fraud participation lie in both greed and the physiological needs of the affected criminals. Engaging fraud from the purview of this category is a product of embarking on a course of action that is relatively more beneficial and less attractive of negative consequences majorly assisted by the anonymity provided by the Internet technology. Participation in fraud therefore, is in line with the existing norm of corrupt related practices and those mostly involved are just cashing on the gap made possible by the today Internet technology. Most importantly is the multiplier effect that the actions of those in the domain of cyber fraud have on international economic cooperation. There is a bleak future for international cooperation if this is not adequately checked and the solution in this regard lies in having the full grasps of cyber fraud evolutionary trend.

Evolution of Cyber Fraud in the Global Community

How did we get to this current level of cyber fraud? This will require the presentation of the chronological account of cyber fraud deducible from the e-commerce environment. However, it is quite unfortunate that there exists dearth of literature on the evolutionary processes that led to and have sustained the current cyber fraud practices globally. The significant contribution that came in handy in the course of writing this paper was that made by Jonathan Clough (2010) and David Montague (2011).

While presenting the evolutionary account of the advent of fraud through the Internet, Clough (2010) explains that the idea of this separate category of computer crimes arose at about the same time that computers became more mainstream. As early as the 1960s, there were reports of computer manipulation, computer sabotage, computer espionage and the illegal use of computer systems (Sieber, 1998:19; Clough, 2010:4). The need to attend to cyber related crimes became more pressing within the period spanning the discoveries of illicit uses of the cyber technology as reported by McKnight (1973) and which Clough (2010) further buttressed by observing that the 70s witnessed concerted attention by stakeholders to the challenges of cyber crime.

Although, Goodman and Brenner (2002) had aptly registered the typologies of crime that pervaded the cyber environment in the 70s, it was specifically observed by Clough that cyber deviance was restricted to the theft of telecommunication services and fraudulent transfer of electronic funds. He stressed that in subsequent decades, the increasing networking of computers and the proliferation of personal computers transformed computer crime and saw the introduction of specific computer crime laws which became another landmark. The major concern of cyber laws in his view involves unauthorized access and economic related crime lately supported by the Internet technology.

Similarly, Montague (2011) argues that the year 1994 heralded the coming of e-commerce and it coincided with a period when the Internet grew in its support for volumes of transaction going on globally. A little further from this period also witnessed the incursions of different types of fraud which occurred on a global scale. The first to be noticed was the use of famous names to commit

fraud. This involves using stolen credit cards to transact business under the cover name of an influential person in the society. The euphoria of the opportunity the Internet offers also blinded users from authenticating the genuineness of the identities of persons in interaction. Cyber fraud in its infancy concentrate on specific targets but thereafter metamorphosed into illegal intrusions affecting sizeable websites.

A more complex strategy involving technical attack followed. Fraudsters brought in the innovation of credit card applications within its potential of bearing real credit card numbers. The credit card was willingly offered online and placed at the disposal of anybody whoever cared. A significant number of fraudsters cash in on this by utilizing the opportunity the card generating applications offer and this was used to conduct searches for available cards online with the intent to effect transactions. As from 1996 onward, fraudsters began to use generated cards for purchases online. This period was marked by tried-and true techniques to get credit card information.

Skimming became rampant, dumpster diving, mail theft, actual theft of people‘s cards and application fraud were handy for the fraud professionals. Succeeding this time was the hunt by fraudsters to harvest credit cards information through hacking into merchant sites, organizational or individuals‘private information with the mind of getting new identities to facilitate the perpetration of fraud directed at innocent people. This technique, called cracking‘became the norm especially for retrieving corporate and personal data. More clever ways of stealing goods and services then opened up and hijacking of consignments meant for rightful owners became rampant.

Consignments were either collected illegally or re-routed by changing delivery notes to the point of convenience to the fraudsters. This growth in fraud that affected the Internet is best succinctly puts in the words of Montague (2011:63) ―as the Internet began to peak in the late 1990s, so did the fraudster‘s creativity in committing fraud. The year I998 progressively witnessed the scrambling for sites by a lot of organizations and business concerns in their quest for relevance and with the hope of appropriating the advantages that the Internet confers. This also translated

to a better harvest period for the fraudsters thus producing in them the capabilities of committing more sophisticated and property scams. Successes were recorded with the innovative efforts deriving from setting up of dummy websites by fraudsters to derail the good intentions of legal users of the Internet.

Worse scenarios were created with the interception of credit cards and private secrets meant to be purportedly routed to many intended destinations. Following from this is the mass theft of identities from the Internet through the information supplied online. With the problems that attended this new development, many organizations and business outfits adopted user account strategy to curtail the incursion of fraud professionals. Interactions were strictly based on marching of what was already known about the users as against their new appearances or request. Despite this steps, Montague disclosed that the fraudster went ahead to circumvent this security provision. Fraudsters began to engage the use of multiplicity of account and the taking over of other people‘s account with modifications. This out rightly occasions the changing of credit card information as many times as they wanted within the 90 days charge back cycle.

On the other hand, fraudster usually take over the account of existing users, change the addresses and place either orders for choice products as what is often preferable to Nigerian youths or request something valuable as in the case of cash. With the advent of auction sites like the eBay and uBid, a lot of fraud schemes arrived and targeted at on-line users according to Montague (2011). Fraudsters went ahead to open rival sites. These sites were used for setting up auction prospects, promoting non-existing goods and services, collecting the payment and changing their identities and thereby converting stolen credit cards to goods and services. By 2000, cyber fraud had attained a clearly defined organized structure with gangs and fraud rings dominating Internet fraud ―business. National rings equally emerged. Montague observed a very systematic attack coordinated to move goods from the sender’s destinations to a third party to sell them emerged. Nigeria is implicated in this regard based on the submission of Montague. Lately, there is the emergence of what he called social engineering which signifies the growth in the boldness of fraudsters in approaching issuing banks, courier services and credit bureaus to complete their fraud. The trend has not changed but is rather growing in sophistication. The account given by

Montague is not exclusive of any geographical boundary but rather it is the clearer picture on how cyber fraud had grown overtime. This will lead us to the next section on the discussion on the incremental rate of cyber fraud and how this implicates the Nigerian youths.

Fraud Multiplication and Youth's Participation in Nigeria

Fraud is not new. Ideally, the taking of property from others has been around as long as man has been on earth. Fraud is characterized as the taking of goods or services from another by use of trick or device (Montague, 2011:59). Although, studies have revealed the wrongfulness or unethical nature of defrauding innocent victims in global business (Tian and Keep, 2002; Dodge, et al, 1996; Fullerton et al, 1996; Muncy and Vitell 1992; Rallapalli et al, 1994; Rawwas et al, 1996; Vitell et al, 1991), current research in Nigeria shows the trend to be on the rise among youths for a good sizeable number of reasons. This position on the rising rate of Internet fraud is consistent with earlier reports on the same issue. Most people believe that fraud is a growing problem. Both the numbers of frauds committed and the total dollar amounts lost to fraud seem to be increasing (Zahra et al, 2007).

Fraud takes different dimension in our generation. With the advent of computers, the Internet, and complex accounting systems, perpetrators now need only to make a telephone call, misdirect purchase invoices, bribe a supplier, manipulate a computer programme, send e-mail or simply push a key on the keyboard to defraud innocent victim or expropriate valuable assets (Tan and Keep, 2002). The strain fraud imposes on economies throughout the world is tremendous. If just one fraud is prevented, billions of dollars can be saved—resources that can be reinvested in building the economy (Albrecht et al, 2012:6). With pragmatic examples, Urbas and Choo (2008) reported that the range of technology-enabled crime is always evolving, both as a function of technological change and in terms of social interaction with new technologies. This change and fraud trend are not unique to Nigeria since before the major concern about youths' involvement in cyber fraud in Nigeria, Morris (2004:20) had earlier expressed apprehension that cyber attacks and fraud would increase exponentially as many more people in the global community decide to participate in or launch into today cyber activities.

The level of vulnerability is equally projected to increase as uses expand. Similarly, the increment in cyber fraud participation had also been anticipated by Cohen and Felson (1979). They argue that crime of diverse kinds will continue to increase under the principle of what they described as the chemistry of crime. This involves the presence or availability of motivated offenders on the one hand, with this category being by expectation jealously supported by endemic opportunities to different planes and the incapacity on the part of the near or affected victims to apprehend the situation, on the other hand. Evidently, the youths represent the motivated offenders, while numerous opportunities available the e-business environment are constantly facilitated by the Internet and the cyber space mysteriously remain uncontrollable either locally or internationally. On all three counts, the digital environment provides fertile ground for the commission and offences (Clough, 2010:5). Situating this in Nigeria‘s context therefore, the motivating factors and the justification for indulging deceitful behaviours stem from such conditions as economic backwardness and social vices rampaging most of the African countries.

Discussing the genesis of cyber fraud in Nigeria, Devine (2011) argues that the now-worldwide Nigerian scam started off as a small, local frauds, in which the con artist would mail out letters informing the victim, or remark, that a prince was looking to deposit a large amount of money in the mark's bank accounts, and would reward him for helping to get the money out of the country. But mailing out letters was expensive and time-consuming, and didn't see the rapid influx of cash to make it anything more than a cottage industry. In giving account on why Nigeria‘s fraud profile assumes current magnitude, Devine has this to say: ‘what truly made the Nigerian version of this age-old trick such a huge industry was the advent of the internet. Modern telecommunications technology and inexpensive internet harvesting software made the Nigerian fraud-mongers able to inexpensively mass-email potential victims. Even if only a small percentage of these people took the bait, the amount of money made could be staggering. And it was. In the past fifteen years, the Nigerian scam went from being a small, local fraud scheme which was essentially a cottage industry, to being one of Nigeria's biggest industries, copied all over the world.’

Further corroborating the efficacy of cyber fraud in Nigeria, Arowosaiye (2008) observes that Nigerian fraudsters and their foreign counterparts are perfect exploiters of the global financial growth and ICT advancement which renders traditional geographical boundaries meaningless. He remarks that today's e-technology makes it possible to transact and plan crime in one country, carry it out in another and move the proceeds from one country to another at the click of a personal computer. This development is not without some remarkable happenings at both local and international level.

Internationally, Bishop and Hydoski (2009) rightly claim that since the Crash of 2008, fraud risks for business and other economic related interactions appear to be on the rise. African nations are not exempted in this regard and it may be said that they are worse off when compared to their counterparts, notably the advanced capitalist nations. Worse off to the extent that a sizeable number of their youths experience the impact of bad economy together with unaccountability in governance locally on the one hand and while such youths do not see prospect of conventional means of making success in life on the other hand. They thereby adopt the cyber medium as a sure money spinning arena in a way. This is also consistent with the theoretical leaning of current research as explicated by Cornish and Clarke (1986) on environmental impact on crime commission. Explaining further on the youths and Internet connections are now breeding fraud. Holland (2010) reports, that computers and the internet technology offer the opportunity for fraud and also reinforce the intent to commit such crime.

Notably, fraudsters have strategic insights that are often supported by material, social and cognitive resources. Material resource manifests in the possession of computer technology, connectivity to the Internet (either through available cyber cafes) and the availability of several software helping fraudulent youths to reach their victims and simultaneously conferring on them the ability to access important information indispensable to the survival of the vulnerable groups. Discussing social resource, this assumes diverse dimensions. In the social realm, the psychological attributes of youths are mainly affected. The peer influence coupled with other factors in the socio-economic environment promoting allurement into anti-social behaviour and the quest to belong which is mostly rampant among youths contribute immensely to the growth

of fraud related activities in Nigeria. Finally, the cognitive attributes include the growing sense of helplessness in the face of the excruciating economic conditions in which a significant number of Third World nations including Nigeria find themselves.

In most cases, frauds are committed through identity faking. In perfecting fraud business/deeds, cyber fraudsters often use false identification to deceive and swindle their clients. Several research and newspaper reports gave insights into the magnitude and the existence of false claims and identification in fraud activism. Iannacci and Morris (2000), for instance, claim however that the use of false identification is not a new problem globally. Evidence show that the annals of criminal law throughout the world and over many years are filled with instances of the use of fraudulent identification documents to assist in carrying out criminal conduct**.** This is more so as there are readily available personal computers, scanners, facsimile machines, Internet access, graphics software, and other technological paraphernalia which possess the ability to produce quality documents of all sorts within the reach of an ever-increasing number of the public (Iannacci and Morris, 2000). Identification fraud is made rife by sophisticated modern technology. The Washington Post (1996:8) has this to say on the role of technology and identification as a means of fraud:

"Due to the increase availability and use of advanced technology, the counterfeiting of documents used to commit crimes or facilitate criminal activity is increasing. There has been an increase in the use of false passports, drivers' licenses, birth certificates and other identification documents. Such documents are used to create a false identity, facilitating illegal immigration, fraud, as well as other criminal activity"

There are three methods of perfecting false identification. These include: acquisition of false identification, some alter or manufacture it while others steal it. In cyber related fraud, these three methods assume prominence.

A significant portion of Nigerian youths as documented in several researches utilize the cyber café in their access to fraud clients. Few of these users lack the expertise needed to present

convincing arguments and documentary back-ups to support the instantiation of fraud business. In order to be successful, they often engage the services of cyber café attendants, fraud mentors or other third party offering such services for a price in the fraud environment that willingly facilitate or supply the missing link. At times, the third-party suppliers of documentation are simply performing their legitimate job, unaware of the inappropriate intentions of the acquirer (Iannacci and Morris, 2000).

In few cases, existing accounts on the Internet are used as baits. These include the intellectual properties represented in scientific, economic, social and psychological eliciting devices needed to dazzle the victims. One of such practices was cited by Jegede (2013), while reporting on an observation witnessed during a field work in a cyber cafés, in which two elderly people engaged the service of a particular expert (cyber café system operator) to assist in copying caterpillars and other excavators cum road construction equipments with the intention of forwarding such pictures to their client in furtherance of their claims of being a drilling firm. Several other fraudsters have their strengths in creating or forging documents with semblance of genuine existing document. They use underground manuals or Google images to achieve better results.

The negative effect of fraud remains colossal at both micro and macro levels. Considering the losses associated with fraud, Budden (1999) argues that fraud exerts the dastard effects on the consumer public at large. It lowers business revenues, which in turn lower the amount of taxes generated to fund public services. Individuals pay more for goods and services as a consequence of fraud and it causes sub optimal allocation of resources for developmental purposes in the larger society (Tian and Keep, 2002). In the same vein, Bishop and Hydoski (2009) argue that fraud drains billions of dollars from the global economy each year. When examining the trend of cyber fraud globally, one may remark that the phenomenon and its sustenance cannot be dissociated from the diverse developments in the socio-economic environment prevailing in most societies.

As a matter of fact, the existence of several typologies of fraud in Nigeria remains incontestable and diverse reasons can also be adduced for its prevalence. Making a detour to the reasons

responsible for the intensification of fraud in Nigeria, one may succinctly situate the core factors institutionalizing fraud in this country under Pedneaut's explanation of fraud intensifiers. He solidly located this in the roles of power and business elites in the modern capitalist economy. Simply put in his words: ―unfortunately, many of the actions of business leaders and politicians have led to a greater acceptance of looking the other way, cutting corners, and cheating the system. Many high-profile cases of fraud or abuse at local, state, and national levels have resulted in little to no consequence to the person responsible, diminishing the perception or threat of any real consequences if anyone else is caught doing the same thing (Pedeanut,2009:20).

All the identified factors represent a positive incentive to fraud. And similarly, if willing to utilize these cues, more people today would commit fraud and go ahead to rationalize their behaviour if they were caught. In Nigeria, staying above board of fraud is now guided by situational ethics (Pedneaut, 2009:20). Estimating the overall effect of this on Nigeria's environment, one may suggest that the youths are seriously affected by the onslaught on our collective values. They are forced consistently and conscientiously to live the life of imitation. Youths rationalize their behaviour by looking at their reference points. Who are they? Those in government they are stealing without being prosecuted or made to account for what they have stolen. They include bulwark of contractors taking contracts without executing them. Body of benchers perverting justice at the reception of bribes and a host of other anomalies implicated in social corruption. The maxim then becomes, if others can, why can't I.

In all known traditional context, youths have been known to be best learners and adopters of innovations. It is basically expected that the comprehensive package of learning and schooling would give the youths both status and a future. However, with the advent of modernity, the tempo of learning and schooling increased tremendously but this came with a price. It soon became glaring that a reckonable number of youths imbibed both the intended (positive) and the unintended (negative) cues through learning. The preference for the unintended can be linked to the growing trend in corrupt related practices across major boundaries of the world. As corruption took the center stage, it is important to note that it simultaneous provided a gamut of stress free opportunities which became handy to a sizeable proportion of youths in most

societies. Consequently, most pragmatic effort directed at restraining or penalizing the youths for making use of any of these or for the adoption of the footsteps of existing corrupt role models became ineffective. This is connected to the erosion of desired values that are needed to keep society in a state of sanity. The linkage between the growing complexity of modern society and the increment in social values displacement has been reported in research (Pedneaut, 2009).

Commenting on the modern society, Pedneaut (2009) argues that crime is accepted by many as the status quo and the modern society as such is devoided of those personal attributes that make for social responsibility such as ethic, moral and pride. In a way, all these desirable attributes have been replaced by greed, self promotion and the ―what is in it for me mentality. Fraud therefore has become easy to execute with modern technologies and the motivation towards participation has equally expanded with the dynamics of modernized society.

Youths are not set out or given to fraud as a way of life, but certain factors and needs in their lives trigger the resolution of becoming fraudulent. It was brought about by share desperation and nurtured by the socio-economic climate pervading most economic backward nation. Just as the e-business environment commands different types of fraud, so also are the people who are into fraud business. The professional fraud artists are conceived as an individual who engages in fraud primarily for monetary or other gains (Jackson, 1994). These artists who are significantly youths engage in fraud in order to survive economically. They cut across all major classes of human society but with variation in the intensity of participation.

In most cases, the family background of most cyber fraudster may be the cause. Research is replete with facts that criminals are usually from lower class families. The impact of bad economy is doubly felt by those at the end of society ladder. However, cyber crime trend globally shows that middle class children are mostly favoured to be successful in online relationship. This assertion is due to the availability and presence of other factors such as possession of requisite education (by both parents and the affected youths), computer literacy (offered by choice schools in Nigeria that children from lower class group may not have access to), affordability of computer gadgets and subscription for the Internet services with the ubiquity

of cell phone which often make access to the Internet less stressful. Holding this constant, the peer influence may contribute or be responsible.

Youths whose families belong to a lower class category may receive a boost from children from middle class family who not only possesses the medium to perpetrate fraud but within the auspices of which lower class youth can receive training. Overall, other factors cannot come into play without the existence of deprivation or poverty often occasioned by the failing society. The initial needs for most fraudsters is often meant to wrest survival but subsequent implications in fraud can be justified when viewed from human nature and drive—greed. Although, the middle class youths was favoured to be more successful in cyber fraud career, it is quite important to note that the bulk of fraud perpetrators in the Internet age consists of economically battered youths who came largely from the working class. This working class category of youths often view themselves as ―outsiders to the society and engage in deceit against their potential victims in retaliation for what they perceive as society‘s unjust treatment of their persons. Despite their predicaments and avowed retaliation on the perceived unjust society, it is often the middle and the upper class youths who provide the enablers in the cyber fraud environment. They supply what is needed to operate successful to most working class youth.

The Essentials of Promoting a fraud Free Environment

With the growth in cyber related fraud and youth's participation globally, it is required of major stakeholders to adopt a far reaching pragmatic solutions toward the reduction and at best eradication of fraud activism. This will involve the amalgam of economic, political, social, legal, cultural and at most religious efforts. Considering these in turn, the economic input is expected to be directed at youth's empowerment. The energies of the ever increasing youth population should be geared towards substantive productive efforts, which can be made realizable through the establishment of productive ventures located in a broad based industrial sector. This will mob-up the wasting potentials of most youths in Nigeria and help harness their contributions to both local and global economy. Politically, the concerted effort of governments across diverse continents is expected to be directed at mustering collective will power to checkmate the insurgence of online fraud. Basically, this would manifest in the promotion of people centric

programmes, eradication of corrupt related practices and the solidification of the economic sector for maximum utilization of labour power and productive engagement of the citizenry. The social aspect for solving the problem of online fraud will entail the collective disapprobation of illegal acquisition of wealth. In this view, the withdrawal of recognition, honour and acceptance of those suspected to be involved the perpetration of fraud and whose actions threatens the consensual basis of human existence will go a long way in discouraging the future resurgence of fraud practices. Legally, most third World nations lack legal instruments needed to eradicate the challenges of the growing online fraud. For instance, Nigeria lacks a functional law formulated or a legal framework upon which to address online fraud so also are many other countries in Africa. It is here suggested that nations in this category should quickly respond to this by filling the gap created by the absence of law since of necessity, the survival of any nation in the current global economic order consists of guaranteeing minimal risk prone environment.

REFERENCES

Albrecht, S. W.. Albrecht, C. O., Albrecht, C. C. and Zimbelman, M. F. (2012) Fraud Examination. Fourth Edition. South-Western: Cengage Learning

Arowosaiye, Y. I. (2008) The New Phenomenon of Phishing, Credit card Fraud, Identity Theft, Internet Privacy and Nigeria Criminal Law. Proceedings except from 3rd Conference of Law and Technology, November, 11-12, ibrahimyusuf@gmail.com

Bishop, T. J. F. and Hydoski, F. E. (2009) Corporate Resilience: Managing the Growing Risk of Fraud and Corruption. Hoboken, New Jersey: John Wiley & Sons.

Budden, Michael C. (1999), Preventing Shoplifting Without Being Sued, Westport, CT: Quorum Books.

Clarke, R.V. and Martin, D.N. (1975) 'A Study of Absconding and its Implications for the Residential Treatment of Delinquents' in J. Tizard, I.A. Sinclair and R.V. Clarke (eds) *Varieties of Residential Experience*. London: Routledge and Kegan Paul.

Clarke, R.V. and Cornish, D.B. (1985) 'Modeling Offenders' Decisions: A Framework for Research and Policy', *Crime and Justice: An Annual Review of Research*, 6: 147–85.

Cohen, L. and Felson, M. (1979). "Social Change and Crime Rates: A Routine Activities Approach." *American Sociological Review*, 44:214-241.

Cornish, D. and Clarke, R.V. (1986) *The Reasoning Criminal*. New York: Springer-Verlag.

Clough, J.. (2010) Principles of Cybercrime. Cambridge: Cambridge University Press.

Dodge, H. R., Edwards, E. A. and Fullerton, S. (1996), "Consumer Transgressions in the Marketplace" Consumers' Perspective," Psychology and Marketing, 13 (December), 821-835.

Devine, J. (2011) History of 419 Internet Fraud. Ezine Articles: file:///C:/Users/jegede/Documents/TheHisrory of 419 Internet Fraud.htm

Ekman, P. (1985), Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage, New York: W.W. Norton & Company.

Fischer2007.DicZeit04.01.2007, http//newsbbc.co.uk/english/static/indepth/uk.2001/lifeofcrime/cybercrimes. (Retrieved June 22, 2010),

Forrester Research www.oscwork.com,au/231/-Australia-Ecommerce-Statistics.html assessed on February 18, 2012.

Fullerton, S., Kerch, K. B. and Dodge, H. R. (1996), Consumer Ethics: An Assessment of Individual Behavior in the Market Place," Journal of Business Ethics, 15 (July), 805-814.

Goodman, M. D. and Brenner, S. W. (2002) 'The emerging consensus on criminal conduct in cyberspace' UCLA Journal of Law and Technology 3, 12.

Holland, G. (2000), I, Mitnick" Village Voice, 45, 7 (February 22), 49, 52

Iannacci, Jerry and Morris, Ron (2000) Access Device Fraud and Related Financial Crime Florida: CRC Press LLC

Jackson, J. E. (1994), Fraud Masters: Professional Credit Card Offenders and Crime," Criminal Justice Review, 19 (Spring), 24-55

Jegede, A.E. (2013) Cyber Fraud Among Youths in Lagos State. Unpublished Doctoral Thesis, Nigeria: Covenant University, Ota, Ogun State.

Kovacich, G. L. (2008) Fighting Fraud: How to Establish and Manage Anti-Fraud Program. UK: Elsevier Academic Press.

McKnight, G. (1973) Computer Crime. London: Joseph.

Montague, D. (2011) Essentials of Online Payment, Security and Fraud Prevention, New Jersey: John Wiley and Sons

Morris, S. (2004) The Future of Netcrime Now: Part 1 - threats and challenges, Home Office Online Report 62/04, p. 20.

Muncy, J. A., and Vitell S. J. (1992), Consumer Ethics: An Investigation of the Ethical Beliefs of the Final Consumer," Journal of Business Research, 24 (June), 297-311.

Pedneaut, S. (2009) Fraud 101: Techniques and Strategies for Understanding Fraud, Third Edition. Hoboken, New Jersey: John Wiley & Co.

Rallapalli, K.C., Vitell, S. J., Wiebe, F. A. and Barnes, J. H. (1994), Consumer Ethical Beliefs and Personality Traits: An Exploratory Analysis," Journal of Business Ethics, 13 (July), 487-495

Rawwas, M., Strutton, D. and Johnson, L. W. (1996), An Exploratory Investigation of the Ethical Values of American and Australian Consumers: Direct Marketing implications," Journal of Direct Marketing, 10 (Autumn), 52-63.

Sieber, U. (1998) Legal Aspects of Computer-Related Crime in the Information Society, COMCRIME Study, European Commission p. 19

Siegel, D. (2008) Diamonds and Organized Crime: The Case of Antwerp in Dina Siegel and Hans Nelen (Eds.) Organized Crime: Culture, Markets and Policies. New York: Springer Science + Business Media

Siegel, L. J. (2010) Criminology: Theories, Patterns and Typologies Tenth Edition, Wadsworth: Cengage Learning.

Singleton, T. W. and Singleton, A. J. (2010) Fraud Auditing and Forensic Accounting, Fourth Edition, New Jersey: John Wiley & Sons, Inc.

Tian, K. and Keep, B. (2002), Customer Fraud and Business Responses: Let the Marketer Beware. Westport CT: Quorum Books.

Urbas, G. and Choo, K. R. (2008) Resource Materials on Technology-Enabled Crime, Technical and Background Paper no. 28 (AIC,), p. 5.

Vitell, S. J., Lumpkin, J. R. and Rawwas, M, Y. (1991), "Consumer Ethics: An Investigation of the Ethical Beliefs of Elderly Consumers," Journal of Business Ethics, 10 (May), 365-375.

Webster's New World Dictionary (1964) College Edition Cleveland and New York: World Publishing: 380.

Well, J. T. (2010) Internet Fraud Casebook: The World Wide Web of Deceit. Hoboken, New Jersey: John Wiley & Sons, Inc.

Zahra, S., Priem, R. and Rasheed, A. (2007) Understanding the Causes and Effects of Top Management Fraud, Organizational Dynamics, Vol. 36: 2.